

MODELO: EVR-100

CONFIGURACIÓN DE TÚNELES VPN PUNTO A PUNTO

SYSCOM, VANGUARDIA EN TECNOLOGÍA

Notas posteriores a la configuración de los EVR-100 para túneles VPN.

1. Los equipos EVR-100 no tienen conexión ADSL directamente, por lo que es necesario utilizar el ruteador ADSL del proveedor como "**Puente**" o "**Bridge**". Para poder establecer la conexión, es necesario tener a la mano el usuario y la contraseña que le proporcione su proveedor de servicio ADSL.

2. Los EVR-100 que se vayan a enlazar en los túneles VPN no pueden tener el mismo segmento LAN, es decir, todos los equipos de fábrica tienen la IP 192.168.0.1; Si quisiéramos enlazar 3 equipos EVR-100 en lugares diferentes, uno debe tener la IP 192.168.0.1, otro la 192.168.1.1 y el último, podría tener la 192.168.2.1 (por ejemplo).

3. Si su servicio ADSL tiene IP Homologada Dinámica (la más común), esto significa que su IP Homologada puede cambiar de un momento a otro sin previo aviso. Para este tipo de condiciones, es necesario contar con una cuenta de **DynDNS**, ya que sin ella, el sistema no será confiable y será necesario estar reconfigurando constantemente los equipos para actualizar las IP Homologadas.

4. Cada EVR-100 debe tener su propio dominio DynDNS, de lo contrario, no funcionará.

5. Es necesario que los datos de la cuenta principal de DynDNS se configuren en el EVR-100 para que éste pueda actualizarla cuando cambie, para que el enlace se mantenga constante.

6. Algunos proveedores de servicios tienen su red con NAT, por lo cual, en algunos casos, no será posible establecer un enlace VPN correctamente.

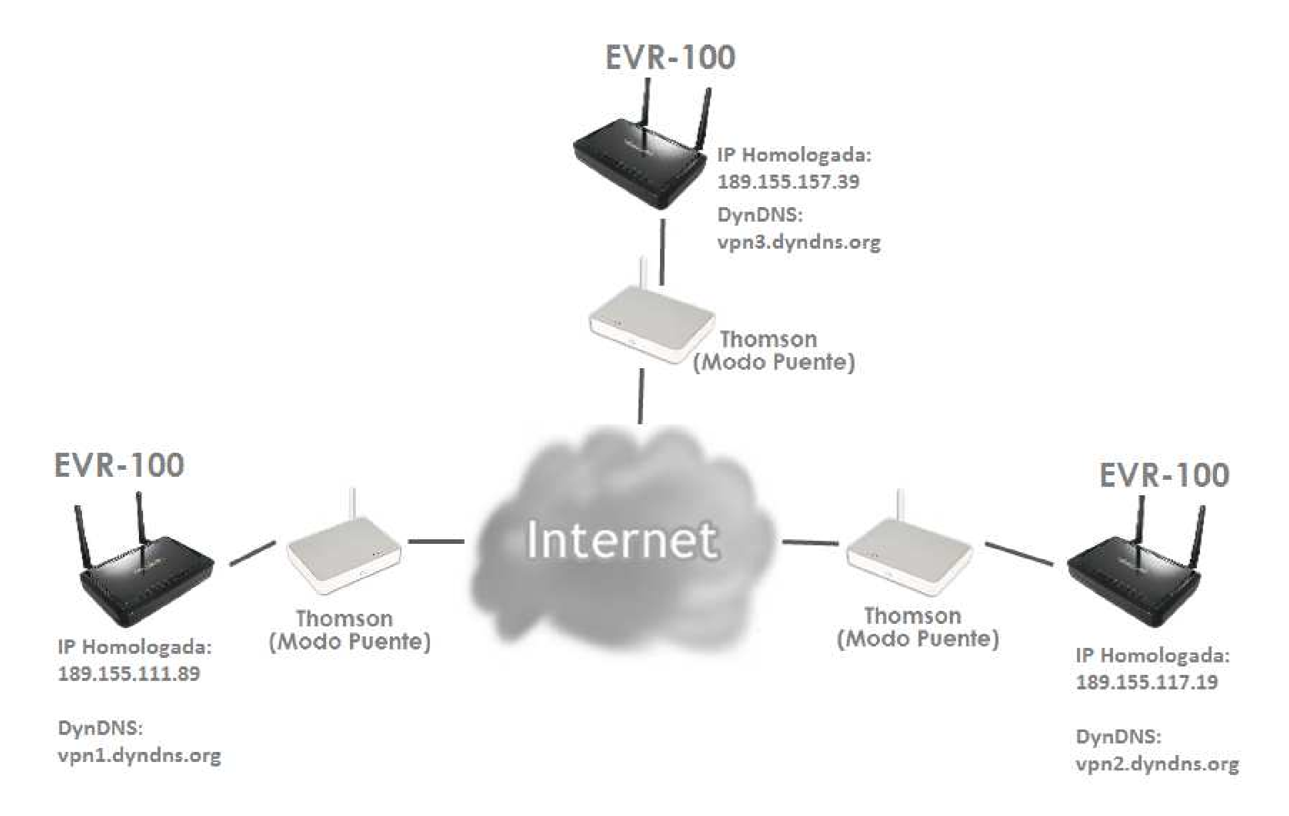
7. No se garantiza la compatibilidad de los túneles VPN con equipos de otras marcas, ya que pueden operar de forma diferente a este sistema. Se recomienda que la red VPN sea de la misma marca.

8. Dependiendo de la **velocidad de bajada y subida** de los servicios de Internet en cada sitio que forma parte de los túneles VPN, el rendimiento o velocidad del sistema puede variar. Se recomienda que los servicios de Internet idénticos de ser posible para que su rendimiento sea simétrico desde y hacia todos los puntos a enlazar.

9. Los túneles VPN permiten enviar Voz por IP (VoIP), radiocomunicación digital de 2 vías (NEXEDGE e IDAS), bases de datos distribuidas en servidores dedicados, entre otros.

10. Si se cuenta con una o más de una **IP Homologada Fija o Estática**, no es necesario utilizar DynDNS.

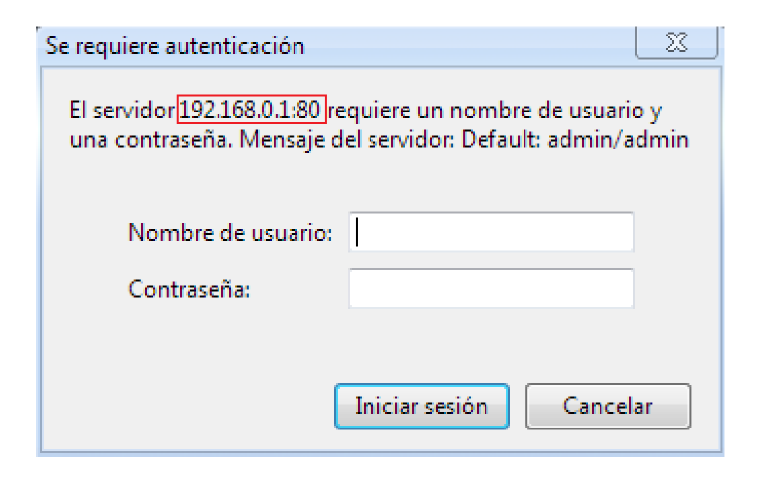
11. El sistema EVR-100 sólo soporta hasta **5 túneles** simultáneos.



En el escenario anterior, cada EVR-100 tiene y actualiza su propio dominio de DynDNS, ya que se asume que todas sus IP Homologadas son **Dinámicas**. Para poder enlazarlos, hay que configurar el protocolo **PPPoE** para que el sistema realice la conexión al proveedor del servicio mediante el **ruteador ADSL en modo puente**.

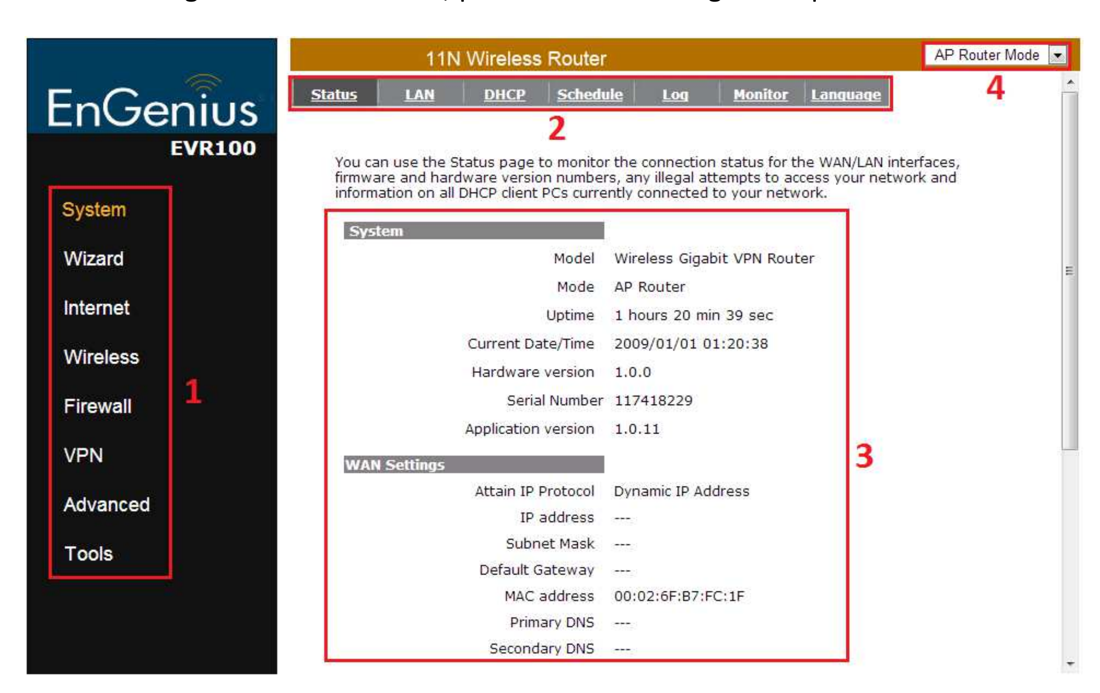
Configuraciones previas para la correcta operación del equipo con túneles VPN.

Para ingresar a las configuraciones del equipo, es necesario abrir el navegador web de su preferencia (se sugiere el uso de Google Chrome o Mozilla Firefox) e ingresar en la barra de direcciones la IP de que le haya sido asignada al equipo después de seguir la guía de configuración básica:



El sistema nos solicitará un usuario y una contraseña, es necesario ingresar: **admin** / **admin** (respectivamente) y presionar el botón "**Iniciar Sesión**"; si el administrador modificó estos parámetros, es necesario introducir el nuevo usuario y la nueva contraseña para acceder.

Una vez dentro de la configuración del sistema, podrá observar la siguiente pantalla:

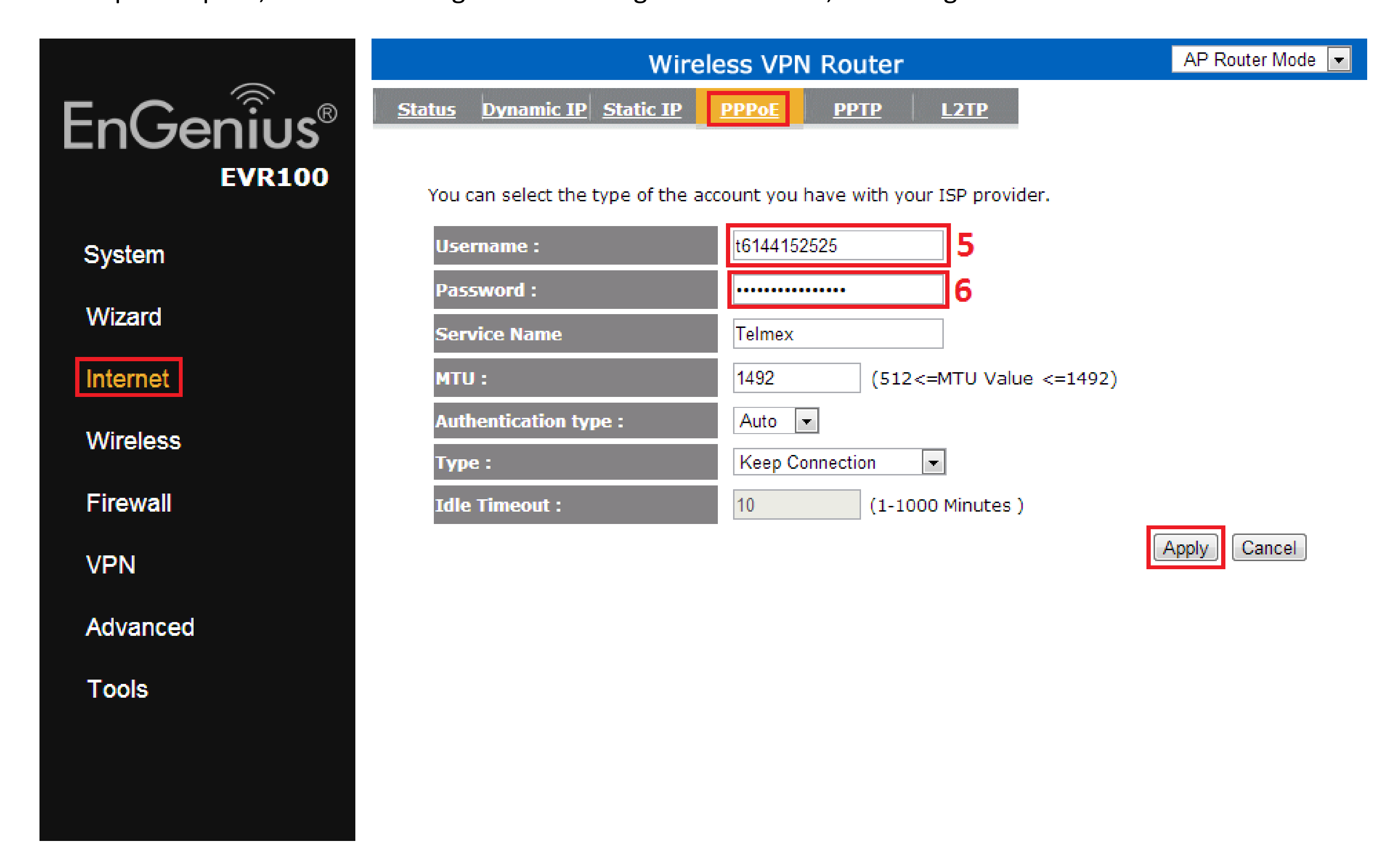


Donde:

1. Categorías Principales de Configuración.
2. Subcategorías.
3. Estado de configuración del sistema (Tiempo encendido, versión de firmware, canal inalámbrico, SSID, tipo de seguridad, etc.).
4. Cambiar modo de operación (AP Router o Universal Repeater).

Al hacer clic sobre cualquier categoría principal, tendremos de lado derecho como pestañas las subcategorías, de las cuales, cada una tiene sus propios parámetros.

Ahora, asumiendo que el equipo ya tiene las configuraciones básicas mencionadas en el otro manual, nos enfocaremos específicamente a la configuración de los parámetros necesarios para las aplicaciones VPN. Como primer paso, es necesario ingresar a la categoría “**Internet**”, sub-categoría “**PPPoE**”.



5. En la casilla "**Username**", es necesario introducir el nombre de usuario que tenemos asignado por parte de nuestro proveedor de servicios ADSL (Telmex, típicamente). Si no cuenta con este dato, es necesario contactar al proveedor del servicio y solicitarlo.

6. En esta casilla, es necesario introducir la contraseña que nos fue asignada por el proveedor para que nuestro ruteador ADSL pueda conectarse a sus servidores. Esta contraseña se la deben proporcionar junto con el nombre de usuario.

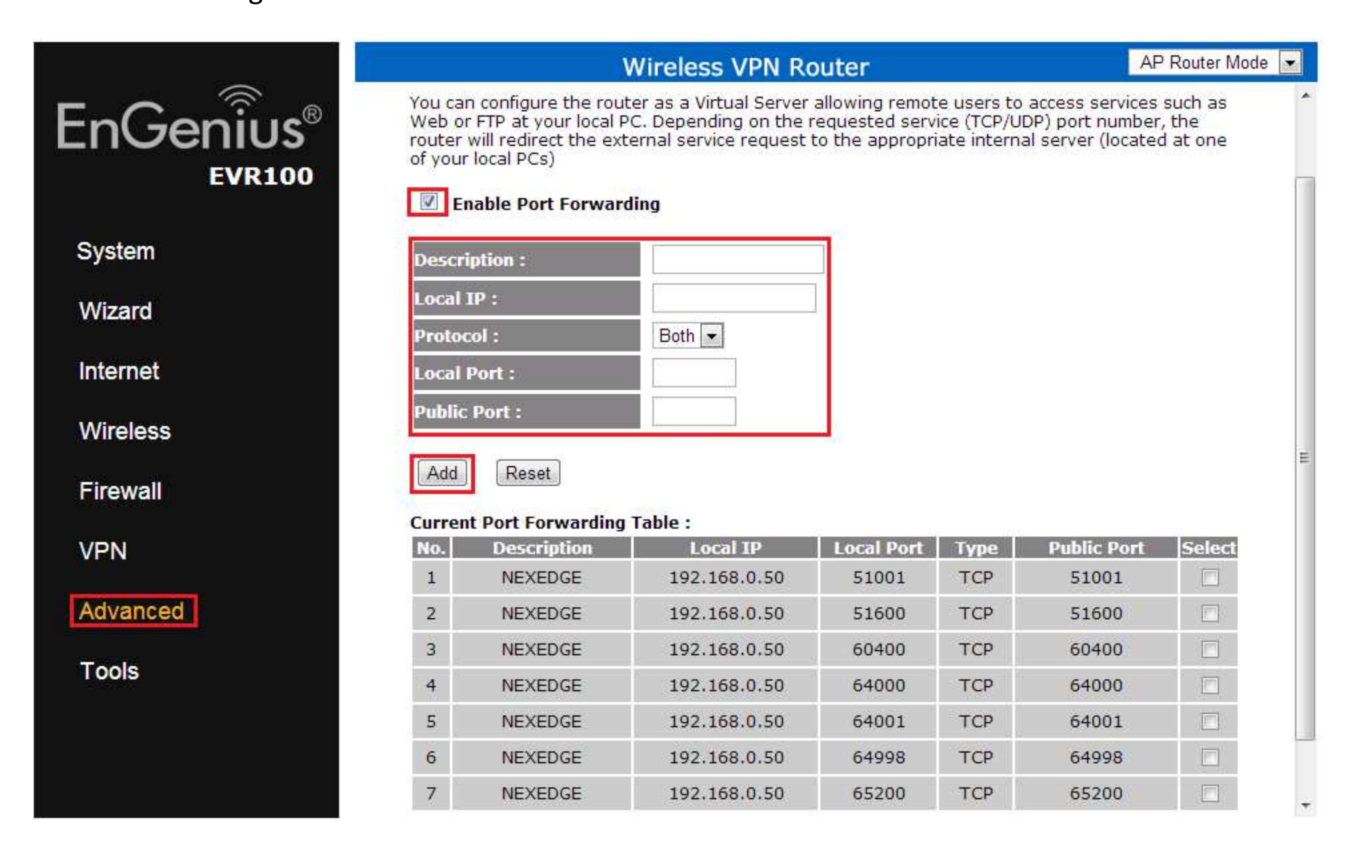
NOTA IMPORTANTE: Se asume que la configuración del ruteador ADSL de los lugares donde esta colocando los EVR-100 ya están configurados en "**Modo Puente**" para la puesta en marcha de las VPN.

Ahora es necesario ingresar a la categoría "**Firewall**", sub-categoría "**Enable**".



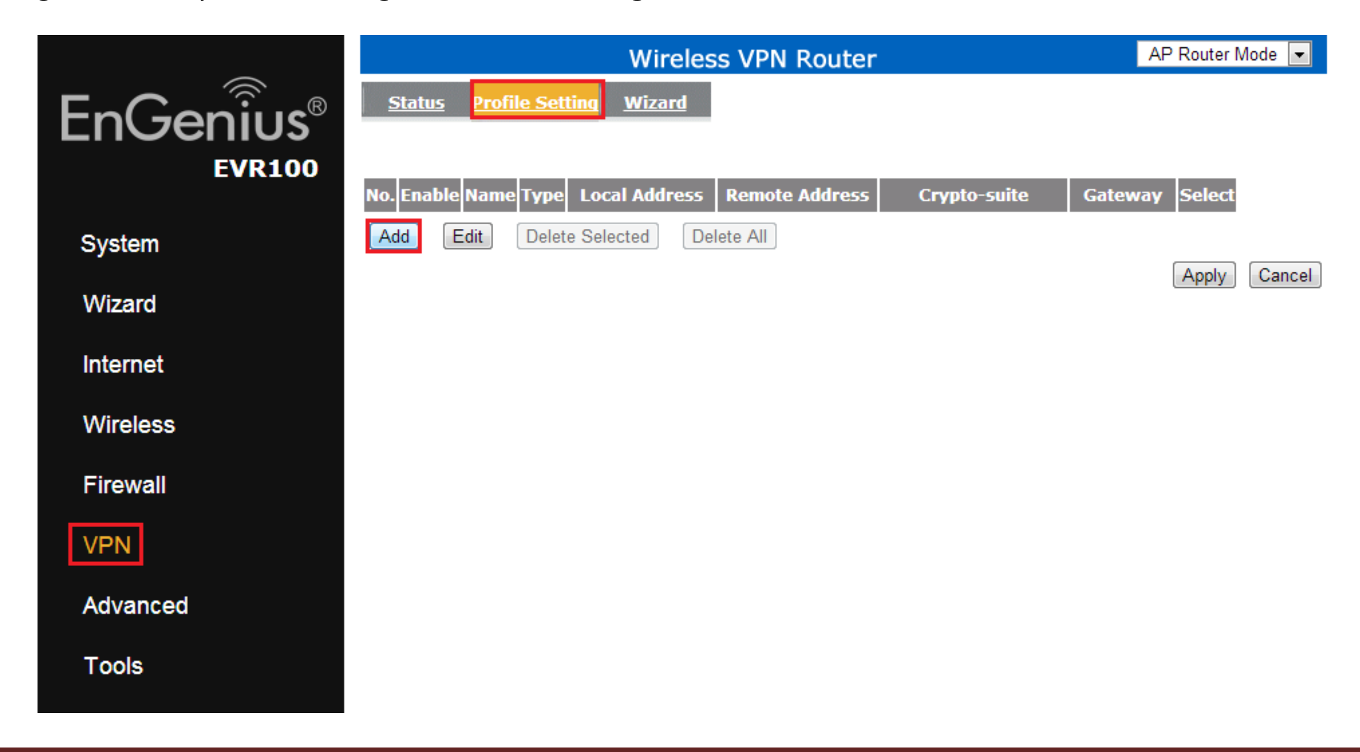
7. Se sugiere desactivar el Firewall (**disable**) del equipo en caso de que desconozca los puertos que debe abrir para sus aplicaciones. En caso contrario, se recomienda que permanezca activado (**enable**) y es necesario rutear los puertos en la categoría "**Advanced**", sub-categoría "**Port FW**".

Veamos a grandes rasgos, la configuración de direccionamiento necesaria para un sistema de radiocomunicación digital **NEXEDGE**:



No.	Description	Local IP	Local Port	Type	Public Port	Select
1	NEXEDGE	192.168.0.50	51001	TCP	51001	
2	NEXEDGE	192.168.0.50	51600	TCP	51600	
3	NEXEDGE	192.168.0.50	60400	TCP	60400	
4	NEXEDGE	192.168.0.50	64000	TCP	64000	
5	NEXEDGE	192.168.0.50	64001	TCP	64001	
6	NEXEDGE	192.168.0.50	64998	TCP	64998	
7	NEXEDGE	192.168.0.50	65200	TCP	65200	

Finalmente, hemos llegado a la parte de la configuración de la (s) VPN. Para esto, es necesario acceder a la categoría “**VPN**” y a la sub-categoría “**Profile Settings**”. Es necesario hacer clic en el botón “**Add**”.

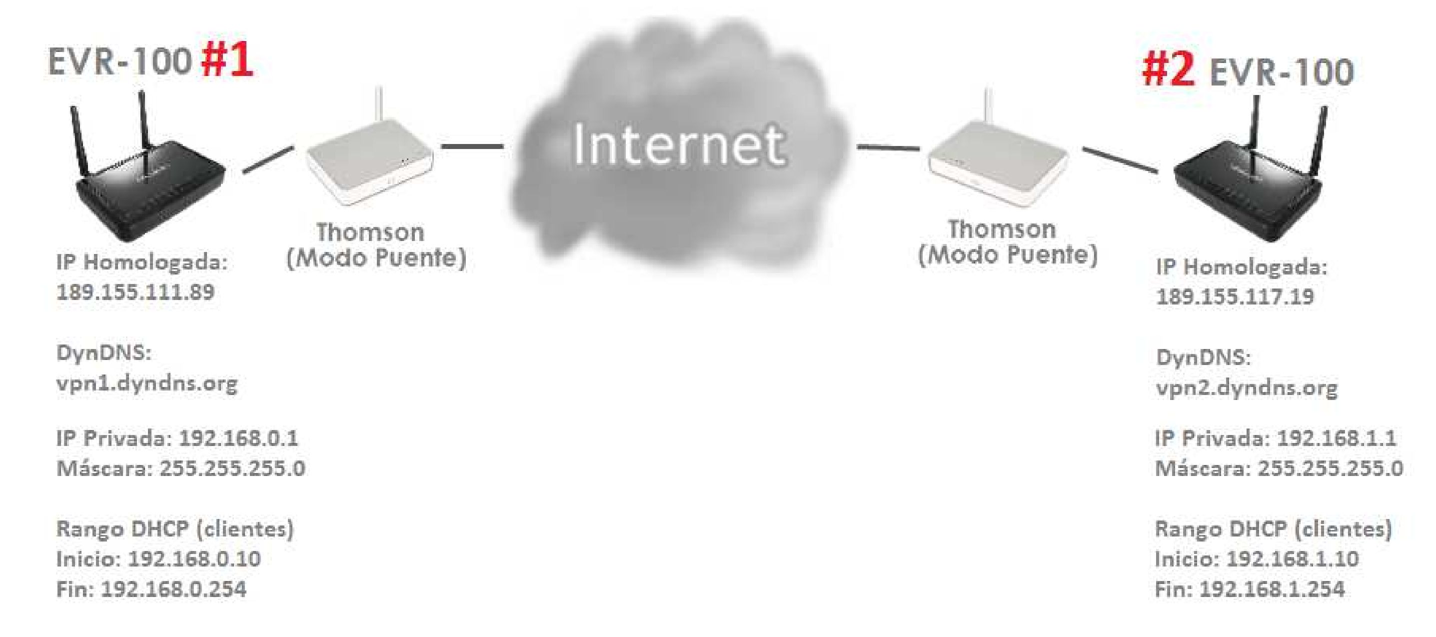


En esta categoría, tendremos 4 subcategorías principales:

- General.
- SA.
- Network.
- Advanced.



Antes de continuar, asumiremos que nuestra aplicación VPN es la siguiente:



Nuestro enlace VPN será entre 2 sitios con IP Homologadas Dinámicas, por lo que utilizaremos DynDNS como nuestro servicio de DDNS para garantizar que el enlace permanecerá activo en todo momento.

La parte de VPN será configurada en 2 partes:

- Configuración del EVR-100 #1.
- Configuración del EVR-100 #2.

CONFIGURACIÓN DEL EVR-100 #1

Sub-categoría “**General**”

Wireless VPN Router — AP Router Mode

General | SA | Network | Advanced

Name :	VPN	8
Connection Type :	IPSec	9
Authentication Type :	pre-shared key	
Shared Key :	clav3SeCrEt4	10
Confirm :	clav3SeCrEt4	
Local ID Type :	Domain Name	11
Local ID :	vpn1.dyndns.org	12
Peer ID Type :	Domain Name	13
Peer ID :	vpn2.dyndns.org	14

Apply | Cancel

8. Primero, hay que asignarle un nombre a nuestro enlace VPN. Se recomienda que el nombre asignado sea igual en ambos equipos EVR-100 (mayúsculas, minúsculas, números, etc.).

9. Aquí tenemos 2 opciones: “**IPSec**” o “**L2TP over IPSec**”; normalmente, cuando la aplicación es Sitio a Sitio (Site-to-Site, como la aplicación que estamos desarrollando), se recomienda que se utilice “**IPSec**”. La conexión “**L2TP over IPSec**” se utiliza típicamente cuando la aplicación es Cliente a Sitio (Client-to-Site), en la cual, usuarios que se encuentran el lugares remotos con acceso a Internet, tienen la capacidad de ingresar a la Intranet de la oficina, donde podría consultar información importante sobre ventas, compras, facturas, pedidos, etc.; siempre y cuando tengan las configuraciones VPN necesarias en sus dispositivos (PC, Laptop, Netbook, Tablet’s, SmartPhones, etc.).

10. La clave secreta o contraseña que utilizaría el túnel VPN para que la conexión y los datos que se manejan sobre ella estén encriptados. Esto garantiza la seguridad de nuestro enlace VPN.

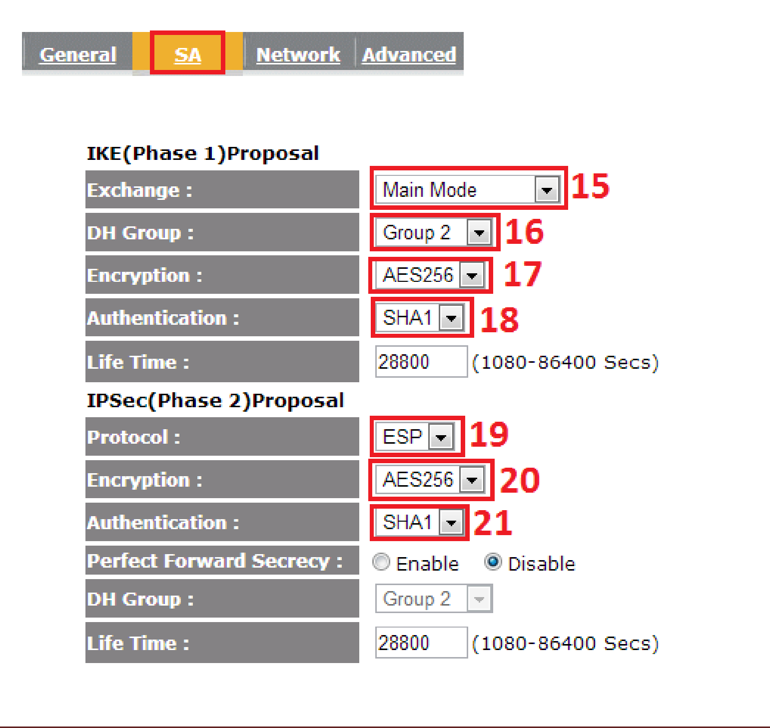
11. El parámetro “**Local ID Type**” se refiere a qué tipo de identificador utilizaremos en nuestro EVR-100 #1, el cual estamos configurando. Las opciones seleccionables con mayor impacto en esta categoría son: “**IP Address**” y “**Domain Name**”. La opción “**IP Address**” sería utilizada si contáramos con una IP Homologada Fija o Estática en nuestro EVR-100 #1; como no es el caso, utilizaremos “**Domain Name**”.

12. Dependiendo de lo que hayamos seleccionado anteriormente, es lo que sería necesario introducir en la sección "**Local ID**", es decir, como seleccionamos "**Domain Name**", debemos introducir el dominio de DynDNS que asignamos específicamente al EVR-100 #1, el cual es: **vpn1.dyndns.org**; si hubiéramos seleccionado "**IP Address**", tendríamos que introducir la IP Homologada Fija o Estática que nos hubiera asignado nuestro proveedor de servicio de Internet.

13. El parámetro "**Peer ID Type**" se refiere a qué tipo de identificador utilizaremos en nuestro EVR-100 #2, el cual estará en el punto remoto. Las opciones seleccionables con mayor impacto en esta categoría son: "**IP Address**" y "**Domain Name**". La opción "**IP Address**" sería utilizada si contáramos con una IP Homologada Fija o Estática en nuestro EVR-100 #2; como no es el caso, utilizaremos "**Domain Name**" también.

14. Dependiendo de lo que hayamos seleccionado anteriormente, es lo que sería necesario introducir en la sección "**Peer ID**", es decir, como seleccionamos "**Domain Name**", debemos introducir el dominio de DynDNS que asignamos específicamente al EVR-100 #2, el cual es: **vpn2.dyndns.org**; si hubiéramos seleccionado "**IP Address**", tendríamos que introducir la IP Homologada Fija o Estática que nos hubiera asignado nuestro proveedor de servicio de Internet.

Finalmente, es necesario hacer clic en el botón "**Apply**" para que se guarden los cambios. Ahora, pasaremos a la subcategoría "**SA**".



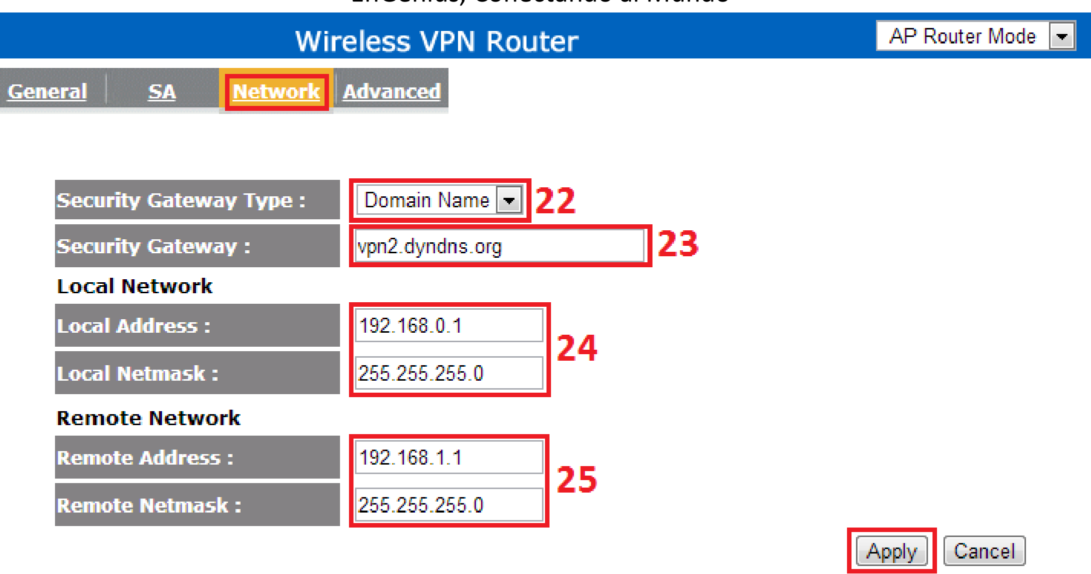
PRIMERA FASE DEL EVR-100 #1

15. El tipo de intercambio (Exchange) nos permite seleccionar 2 modos de conexión para la primera fase de la VPN: “**Main Mode**” y “**Aggressive Mode**”; “**Main Mode**” es por defecto, la opción predefinida, ya que utiliza los estándares de negociación requeridos para la conexión, brindando una mejor estabilidad y seguridad. El modo “**Aggressive Mode**”, intenta establecer la conexión en tiempos muy cortos, sin esperar el tiempo requerido por los estándares utilizados, lo que hace a este modo una conexión insegura e inestable.
16. El parámetro “**DH Group**” nos permite incrementar la seguridad de nuestra VPN en su fase 1. Entre más elevado es el valor del grupo, es más alto el nivel de seguridad. Se recomienda utilizar como predeterminado el “**Group 2**”.
17. El equipo EVR-100 es compatible con los siguientes tipos de seguridad: **DES, 3DES, AES-128, AES-192, AES-256** o puede incluso no tener seguridad (**none / disabled**), lo cual no se recomienda. Dependiendo del tipo de información que se vaya a trabajar sobre la VPN, se recomienda utilizar una clave convencional (**DES**) o una de alto nivel (**AES**).
18. El método de autenticación de la fase 1 permite seleccionar 2 opciones: “**MD5**” o “**SHA1**”. Ambos métodos de autenticación son bastante confiables, pero se recomienda utilizar como predeterminado el método “**SHA1**”.

SEGUNDA FASE DEL EVR-100 #1

19. El protocolo de la fase 2 de la conexión VPN nos brinda las siguientes 2 opciones: “**ESP**” o “**AH**”; el protocolo “**ESP**” garantiza una mejor integridad de los datos, verificación de datos desde el origen y un nivel de confidencialidad mejorado, mientras que el protocolo “**AH**” sólo verifica los datos desde el origen. Se recomienda utilizar por defecto el protocolo “**ESP**”.
20. El equipo EVR-100 es compatible con los siguientes tipos de seguridad: **DES, 3DES, AES-128, AES-192, AES-256** o puede incluso no tener seguridad (**none / disabled**), lo cual no se recomienda. Dependiendo del tipo de información que se vaya a trabajar sobre la VPN, se recomienda utilizar una clave convencional (**DES**) o una de alto nivel (**AES**).
21. El método de autenticación de la fase 2 permite seleccionar las mismas 2 opciones de la fase 1: “**MD5**” o “**SHA1**”. Ambos métodos de autenticación son bastante confiables, pero se recomienda utilizar como predeterminado el método “**SHA1**”.

Ahora nos desplazaremos hasta la sub-categoría “**Network**” para configurar el direccionamiento entre ambos equipos EVR-100.



22. Este parámetro (Security Gateway Type), tiene varias formas de validación: "**IP Address**" o "**Domain Name**"; típicamente, dependiendo de lo que se haya configurado en la sub-categoría "**General**", este parámetro es el mismo que el "**Peer ID Type**", el cual sería en este caso "**Domain Name**".

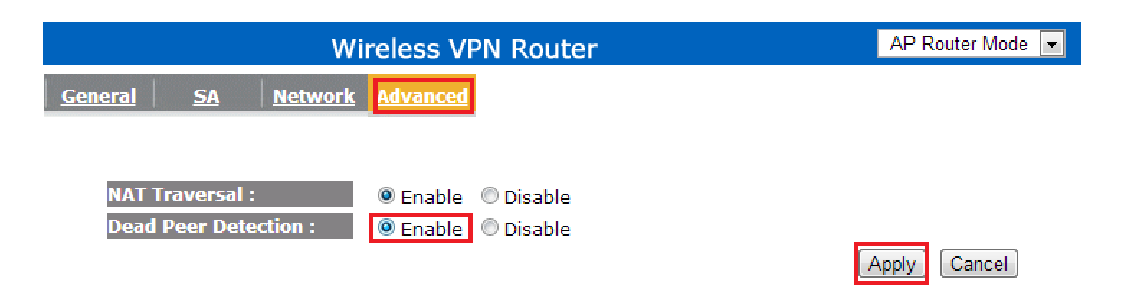
23. Este parámetro (Security Gateway Type), tiene varias formas de validación: "**IP Address**" o "**Domain Name**"; típicamente, dependiendo de lo que se haya configurado en la sub-categoría "**General**", este parámetro es el mismo que el "**Peer ID**", el cual sería en el caso del EVR-100 #1: **vpn2.dyndns.org**

24. Los parámetros "**Local Address**" y "**Local Netmask**" corresponden a la IP local o privada del EVR-100 #1 (192.168.0.1) y su respectiva máscara de subred (255.255.255.0). Se recomienda consultar el diagrama de conexión propuesto en la ***página 8*** como referencia.

25. Los parámetros "**Remote Address**" y "**Remote Netmask**" corresponden a la IP local o privada del EVR-100 #2 (192.168.1.1) y su respectiva máscara de subred (255.255.255.0). Se recomienda consultar el diagrama de conexión propuesto en la ***página 8*** como referencia.

Finalmente, presionamos nuevamente el botón "**Apply**" para aplicar cambios.

En la última sub-categoría de la configuración VPN del EVR-100 #1 (**Advanced**), sólo basta con activar la función "**Dead Peer Detection**" para que el equipo detecte si se cae la conexión e intente conectarse nuevamente.



Sub-categoría "**General**"

General | SA | Network | Advanced

Name :	VPN	26
Connection Type :	IPSec	27
Authentication Type :	pre-shared key	
Shared Key :	clav3SeCrEt4	28
Confirm :	clav3SeCrEt4	
Local ID Type :	Domain Name	29
Local ID :	vpn2.dyndns.org	30
Peer ID Type :	Domain Name	31
Peer ID :	vpn1.dyndns.org	32

Apply Cancel

26. Primero, hay que asignarle un nombre a nuestro enlace VPN. Se recomienda que el nombre asignado sea igual en ambos equipos EVR-100 (mayúsculas, minúsculas, números, etc.).

27. Aquí tenemos 2 opciones: "**IPSec**" o "**L2TP over IPSec**"; normalmente, cuando la aplicación es Sitio a Sitio (Site-to-Site, como la aplicación que estamos desarrollando), se recomienda que se utilice "**IPSec**". La conexión "**L2TP over IPSec**" se utiliza típicamente cuando la aplicación es Cliente a Sitio (Client-to-Site), en la cual, usuarios que se encuentran el lugares remotos con acceso a Internet, tienen la capacidad de ingresar a la Intranet de la oficina, donde podría consultar información importante sobre ventas, compras, facturas, pedidos, etc.; siempre y cuando tengan las configuraciones VPN necesarias en sus dispositivos (PC, Laptop, Netbook, Tablet's, SmartPhones, etc.).

28. La clave secreta o contraseña que utilizaría el túnel VPN para que la conexión y los datos que se manejan sobre ella estén encriptados. Esto garantiza la seguridad de nuestro enlace VPN.

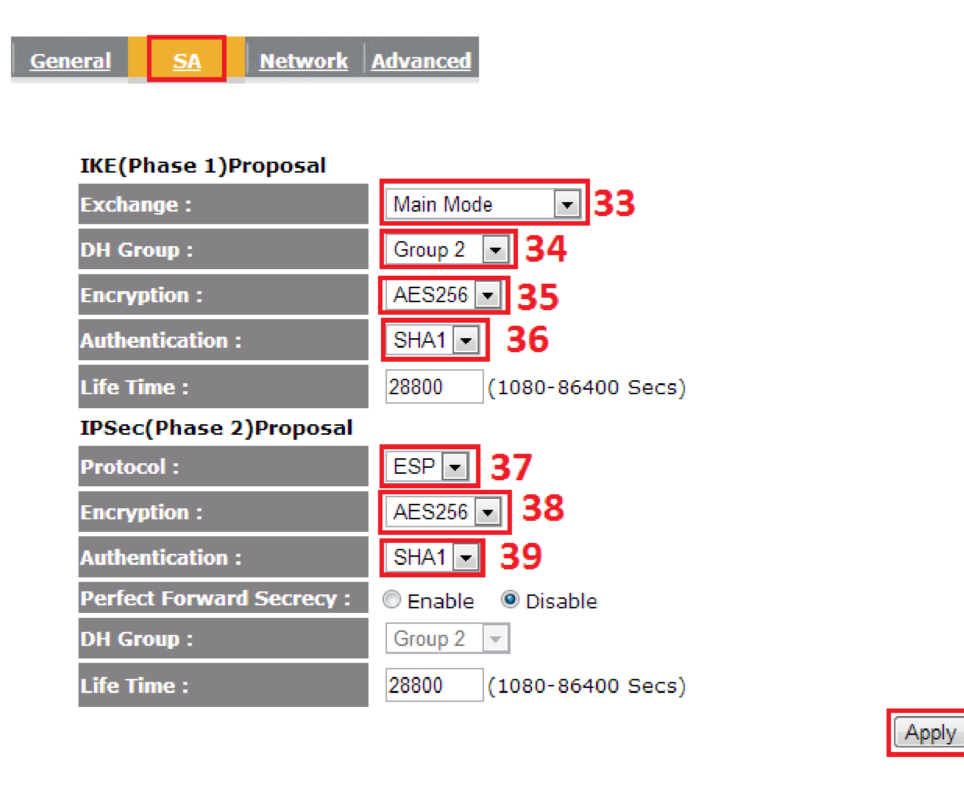
29. El parámetro "**Local ID Type**" se refiere a qué tipo de identificador utilizaremos en nuestro EVR-100 #2, el cual estamos configurando. Las opciones seleccionables con mayor impacto en esta categoría son: "**IP Address**" y "**Domain Name**". La opción "**IP Address**" sería utilizada si contáramos con una IP Homologada Fija o Estática en nuestro EVR-100 #1; como no es el caso, utilizaremos "**Domain Name**".

30. Dependiendo de lo que hayamos seleccionado anteriormente, es lo que sería necesario introducir en la sección “**Local ID**”, es decir, como seleccionamos “**Domain Name**”, debemos introducir el dominio de DynDNS que asignamos específicamente al EVR-100 #2, el cual es: **vpn2.dyndns.org**; si hubiéramos seleccionado “**IP Address**”, tendríamos que introducir la IP Homologada Fija o Estática que nos hubiera asignado nuestro proveedor de servicio de Internet.

31. El parámetro “**Peer ID Type**” se refiere a qué tipo de identificador configuramos en nuestro EVR-100 #1, el cual esta en el punto remoto. Las opciones seleccionables con mayor impacto en esta categoría son: “**IP Address**” y “**Domain Name**”. La opción “**IP Address**” sería utilizada si contáramos con una IP Homologada Fija o Estática en nuestro EVR-100 #1; como no es el caso, utilizaremos “**Domain Name**” también.

32. Dependiendo de lo que hayamos seleccionado anteriormente, es lo que sería necesario introducir en la sección “**Peer ID**”, es decir, como seleccionamos “**Domain Name**”, debemos introducir el dominio de DynDNS que asignamos específicamente al EVR-100 #1, el cual es: **vpn1.dyndns.org**; si hubiéramos seleccionado “**IP Address**”, tendríamos que introducir la IP Homologada Fija o Estática que nos hubiera asignado nuestro proveedor de servicio de Internet.

Finalmente, es necesario hacer clic en el botón “**Apply**” para que se guarden los cambios. Ahora, pasaremos a la subcategoría “**SA**”.



PRIMERA FASE DEL EVR-100 #2

33. El tipo de intercambio (Exchange) nos permite seleccionar 2 modos de conexión para la primera fase de la VPN: "**Main Mode**" y "**Aggressive Mode**"; "**Main Mode**" es por defecto, la opción predefinida, ya que utiliza los estándares de negociación requeridos para la conexión, brindando una mejor estabilidad y seguridad. El modo "**Aggressive Mode**", intenta establecer la conexión en tiempos muy cortos, sin esperar el tiempo requerido por los estándares utilizados, lo que hace a este modo una conexión insegura e inestable.

34. El parámetro "**DH Group**" nos permite incrementar la seguridad de nuestra VPN en su fase 1. Entre más elevado es el valor del grupo, es más alto el nivel de seguridad. Se recomienda utilizar como predeterminado el "**Group 2**".

35. El equipo EVR-100 es compatible con los siguientes tipos de seguridad: **DES, 3DES, AES-128, AES-192, AES-256** o puede incluso no tener seguridad (**none / disabled**), lo cual no se recomienda. Dependiendo del tipo de información que se vaya a trabajar sobre la VPN, se recomienda utilizar una clave convencional (**DES**) o una de alto nivel (**AES**).

36. El método de autenticación de la fase 1 permite seleccionar 2 opciones: "**MD5**" o "**SHA1**". Ambos métodos de autenticación son bastante confiables, pero se recomienda utilizar como predeterminado el método "**SHA1**".

SEGUNDA FASE DEL EVR-100 #2

37. El protocolo de la fase 2 de la conexión VPN nos brinda las siguientes 2 opciones: "**ESP**" o "**AH**"; el protocolo "**ESP**" garantiza una mejor integridad de los datos, verificación de datos desde el origen y un nivel de confidencialidad mejorado, mientras que el protocolo "**AH**" sólo verifica los datos desde el origen. Se recomienda utilizar por defecto el protocolo "**ESP**".

38. El equipo EVR-100 es compatible con los siguientes tipos de seguridad: **DES, 3DES, AES-128, AES-192, AES-256** o puede incluso no tener seguridad (**none / disabled**), lo cual no se recomienda. Dependiendo del tipo de información que se vaya a trabajar sobre la VPN, se recomienda utilizar una clave convencional (**DES**) o una de alto nivel (**AES**).

39. El método de autenticación de la fase 2 permite seleccionar las mismas 2 opciones de la fase 1: "**MD5**" o "**SHA1**". Ambos métodos de autenticación son bastante confiables, pero se recomienda utilizar como predeterminado el método "**SHA1**".

Ahora nos desplazaremos hasta la sub-categoría "**Network**" para configurar el direccionamiento entre ambos equipos EVR-100.

Wireless VPN Router   AP Router Mode

General | SA | Network | Advanced

Security Gateway Type :	Domain Name (40)
Security Gateway :	vpn1.dyndns.org (41)
Local Network	
Local Address :	192.168.1.1 (42)
Local Netmask :	255.255.255.0
Remote Network	
Remote Address :	192.168.0.1 (43)
Remote Netmask :	255.255.255.0

Apply   Cancel

40. Este parámetro (Security Gateway Type), tiene varias formas de validación: "**IP Address**" o "**Domain Name**"; típicamente, dependiendo de lo que se haya configurado en la sub-categoría "**General**", este parámetro es el mismo que el "**Peer ID Type**", el cual sería en este caso "**Domain Name**".

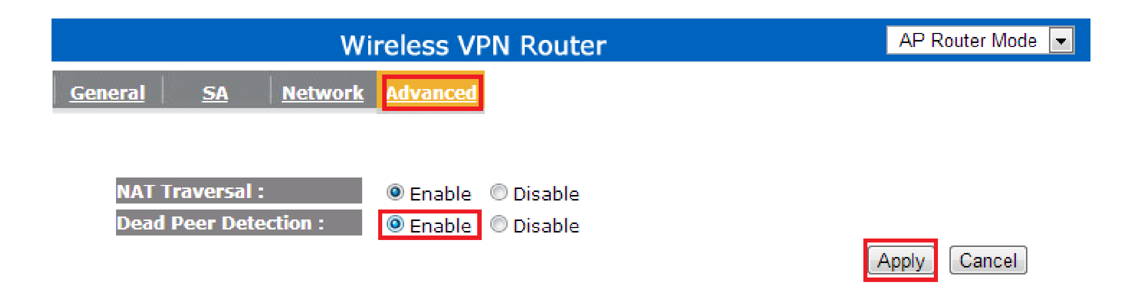
41. Este parámetro (Security Gateway Type), tiene varias formas de validación: "**IP Address**" o "**Domain Name**"; típicamente, dependiendo de lo que se haya configurado en la sub-categoría "**General**", este parámetro es el mismo que el "**Peer ID**", el cual sería en el caso del EVR-100 #2: **vpn1.dyndns.org**

42. Los parámetros "**Local Address**" y "**Local Netmask**" corresponden a la IP local o privada del EVR-100 #2 (192.168.1.1) y su respectiva máscara de subred (255.255.255.0). Se recomienda consultar el diagrama de conexión propuesto en la ***página 8*** como referencia.

43. Los parámetros "**Remote Address**" y "**Remote Netmask**" corresponden a la IP local o privada del EVR-100 #1 (192.168.0.1) y su respectiva máscara de subred (255.255.255.0). Se recomienda consultar el diagrama de conexión propuesto en la ***página 8*** como referencia.

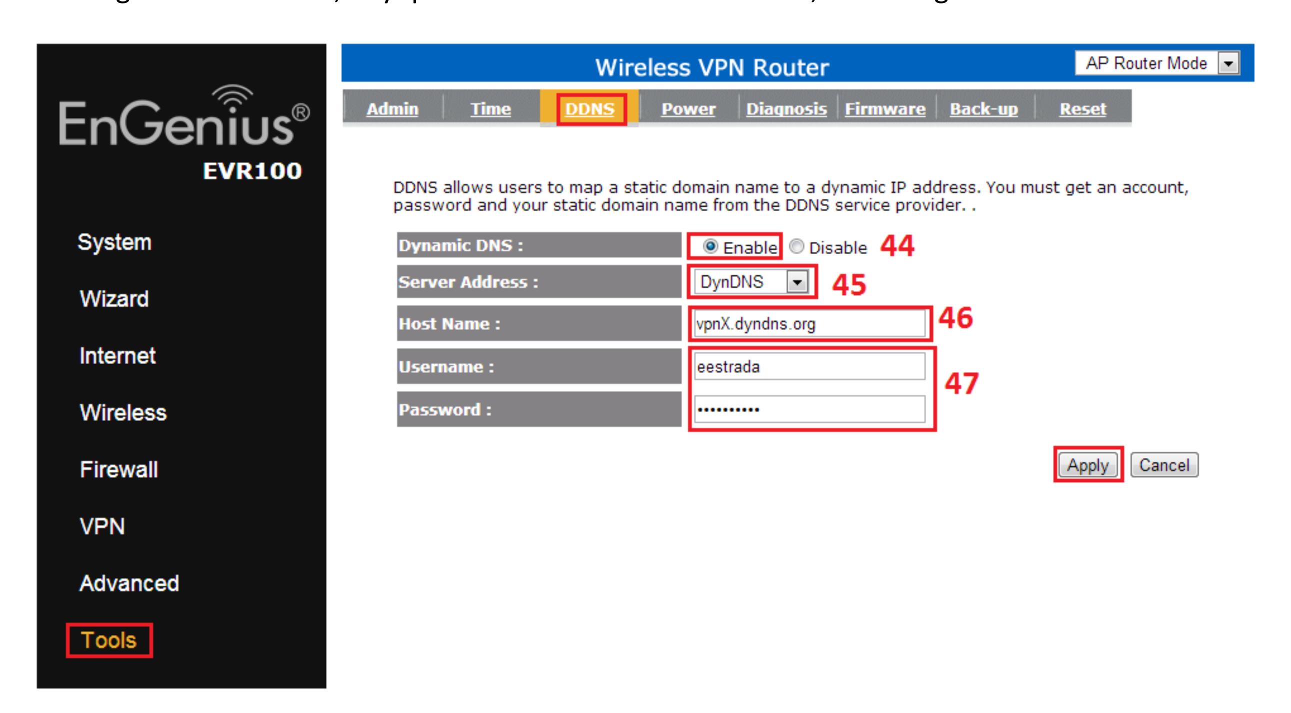
    Finalmente, presionamos nuevamente el botón "**Apply**" para aplicar cambios.

En la última sub-categoría de la configuración VPN del EVR-100 #2 (**Advanced**), sólo basta con activar la función "**Dead Peer Detection**" para que el equipo detecte si se cae la conexión e intente conectarse nuevamente.



Para concluir este manual, no hay que olvidar configurar los datos de la cuenta de DynDNS en ambos equipos EVR-100, ya que si no se configuran los datos requeridos, los equipos no actualizarán la IP Homologada Dinámica cada vez que se la cambie el proveedor.

Para configurar estos datos, hay que acceder a la sección "**Tools**", sub-categoría "**DDNS**".



44. Hay que habilitar (Enable) la función DDNS para que nos permita configurar los demás parámetros.

45. Aquí debemos seleccionar el proveedor de servicios DDNS que utilizaremos, de los cuales, el más conocido y utilizado es "**DynDNS**".

46. Aquí debemos introducir la dirección que creamos en la cuenta de DynDNS para los EVR-100 (según corresponda), donde:

    EVR-100 #1: vpn1.dyndns.org

    EVR-100 #2: vpn2.dyndns.org

47. Estos datos corresponden a los de nuestra cuenta con **DynDNS**, es decir, el usuario y la contraseña con la que accedemos a la página de DynDNS para administrar nuestros dispositivos.

Después de finalizar todos los pasos anteriores, nuestros equipos ya están listos para operar, sólo queda realizar las pruebas pertinentes de conexión para garantizar que nuestros servicios están disponibles y podemos ver los nodos remotos desde la red local.